MICHAEL W. BIEN – 096891
ERNEST GALVAN – 196065
VAN SWEARINGEN – 259809
BENJAMIN BIEN-KAHN – 267933
ALEXANDER GOURSE – 321631
AMY XU – 330707
ROSEN BIEN
GALVAN & GRUNFELD LLP
101 Mission Street, Sixth Floor
San Francisco, California 94105-1738
Telephone: (415) 433-6830
Facsimile: (415) 433-7104
Email: mbien@rbgg.com
egalvan@rbgg.com
vswearingen@rbgg.com
bbien-kahn@rbgg.com
agourse@rbgg.com
axu@rbgg.com

KELIANG (CLAY) ZHU – 305509
DEHENG LAW OFFICES PC
7901 Stoneridge Drive #208
Pleasanton, California 94588
Telephone: (925) 399-5856
Facsimile: (925) 397-1976
Email: czhu@dehengsv.com

ANGUS F. NI – Admitted *Pro Hac Vice*
AFN LAW PLLC
502 Second Avenue, Suite 1400
Seattle, Washington 98104
Telephone: (773) 543-3223
Email: angus@afnlegal.com

THOMAS R. BURKE – 141930
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street, Suite 800
San Francisco, California 94111-6533
Telephone: (415) 276-6500
Facsimile: (415) 276-6599
Email: thomasburke@dwt.com

DAVID M. GOSSETT – Admitted *Pro Hac Vice*
DAVIS WRIGHT TREMAINE LLP
1301 K Street N.W., Suite 500 East
Washington, D.C. 20005-3366
Telephone: (202) 973-4216
Facsimile: (202) 973-4499
Email: davidgossett@dwt.com

JOHN M. BROWNING – *Pro Hac Vice* forthcoming
DAVIS WRIGHT TREMAINE LLP
1251 Avenue of the Americas, 21st Floor
New York, New York 10020-1104
Telephone: (212) 603-6410
Facsimile: (212) 483-8340
Email: jackbrowning@dwt.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE, CHIHUO INC., BRENT COULTER, FANGYI DUAN, JINNENG BAO, ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official capacity as President of the United States, and WILBUR ROSS, in his official capacity as Secretary of Commerce,

Defendants.

Case No. 3:20-cv-05910-LB

DECLARATION OF JOE HILDEBRAND IN SUPPORT OF PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO STAY PENDING APPEAL OF ORDER GRANTING MOTION FOR PRELIMINARY INJUNCTION

Date: October 15, 2020
Time: 9:30 a.m.
Crtrm.: Remote

Judge: Hon. Laurel Beeler
Trial Date: None Set

I, Joe Hildebrand, declare as follows:

1. I am an expert with 30-years' experience in soft development, data security, and related fields. I have been asked by plaintiffs' counsel to provide my expert opinion in this case concerning the Government's effort to ban or restrict WeChat in the United States. I worked for Cisco for 8 years (2008 to 2016), reaching the rank of Distinguished Engineer. Cisco is the worldwide leader in IT, networking, and cybersecurity solutions. As part of the management team of Cisco, I was responsible for the technical direction of a highly-scalable multi-protocol instant messaging software product with various storage back-ends, developed prototypes and production code in C, C++, C#, Java, Perl, Python, and Delphi on Linux, Solaris, Mac, and Windows, provided final escalation point for all technical problems in Development, Professional Services, and Support, participated in the formation of corporate-wide and Internet-wide technology strategy, served as the chief architect for Cisco's cloud collaboration applications group, including WebEx Meetings, Messenger, and related products, and provided technical liaison for industry analysts and reporters through briefings, whitepapers, and industry conferences.

2. In addition to my tenure with Cisco, I served various senior technical positions for companies including Jabber (an Instant Messaging company acquired by Cisco), Time Warner and Interlink. Most recently, I worked for Mozilla from October 2016 to August 2020, responsible for the entire engineering team – 700 people spread all over the world – for a major web browser, Firefox.

3. I served on the board of directors of the Internet Security Research Group (ISRG) in 2016. ISRG is the non-profit organization behind Let's Encrypt, one of the largest Certificate Authorities in the world. I remain on their Technical Advisory Board.

4. I served on the Internet Architecture Board (IAB) for 4 years (2014-2018). The IAB is a non-governmental agency that provides long-range technical direction for Internet development, and a management function for the standards processes pursued by the Internet Engineering Task Force (IETF). As a part of my IETF participation, I managed the eXtensible Messaging and Presence Protocol (XMPP) working group, the HyBi working group (which produced WebSockets), and the WebPush working group. I have contributed to numerous standards documents there.

5. Of all my previous experiences, cyber security and data privacy are an important and constant topic, and I have accumulated extensive expertise. My recent CV is attached.

6. I have personal knowledge of the matters stated herein and if called as a witness I could and would testify truthfully to them.

7. In general, data security is achieved through tradeoffs among three core objectives: confidentiality, integrity, and availability of data.[1] It is an exercise in risk management, including the identification, assessment, and mitigation of risks to acceptable levels at an appropriate cost. In addition, when it comes to data security threats, it is virtually impossible to prove the negative and that there are no risks to a particular network or software.[2] Technology is always evolving, and will reveal existing or new vulnerabilities. Even the best companies in the world cannot claim that no data risks exist for their networks or systems.

[1] The three security objectives are discussed by the National Institute of Standards and Technology, FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems", at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[2] Shuman Ghosemajumder, You Can't Secure 100% of Your Data 100% of The Time, Harvard Business Review (Dec. 4, 2017), at https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time.

8. Accordingly, the industry has developed a set of best practices for mitigating data security risk.[3] Some of the core measures include segmenting and tightly controlling access to a company's sensitive data, maintaining and auditing access logs to detect and address any deviations from expected behaviors including unauthorized access, and encrypting user data in storage and during transmission in such a way that access to data transiting a system would be extremely difficult ("end-to-end encryption").

9. These best practices have not been fully adopted among major companies in the U.S. These companies have made the different tradeoffs among the three core objectives – confidentiality, integrity, and availability of data – and have achieved different levels of security while paying attention to cost, user experience, and other factors. Moreover, the U.S. government is fighting against end-to-end encryption, and has undermined the industry's effort to achieve better security.[4] As a result, the American companies themselves do not have a good track record of protecting user data, as incidents of large-scale data leaks and breaches are recurring in the news.

10. I have read the Executive Order issued on August 6, 2020 that bans the use of WeChat in the U.S. If the Executive Order is truly concerned about the threat that the Chinese government may access the data of the WeChat users in the U.S., there are targeted measures based on industry best practices that can effectively address such a concern. First of all,

[3] *See* Federal Trade Commission, Start with Security (June 2015); Thomas B. Pahl, Stick with Security: Segment your network and monitor who's trying to get in and out (Aug. 25, 2017), at https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-segment-your-network-monitor-whos-trying-get; National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (April 16, 2018).

[4] DOJ has been trying to force Facebook to give up end-to-end encryption, and Congress is considering bills to cripple end-to-end encryption with the support of DOJ. See https://www.pcmag.com/news/gop-senators-try-to-cripple-end-to-end-encryption-with-new-bill and https://nakedsecurity.sophos.com/2019/12/12/facebook-refuses-to-break-end-to-end-encryption/.

partnering with a U.S. cloud provider for user data storage. This will provide a relatively secure place for user data and also allow easy audit and oversight to detect unauthorized data access. Secondly, regular compliance audits and notifications, which should be a part of almost any set of mitigations. Thirdly, stringent corporate or even external oversight over management and personnel with access to user data, which is industry best practice. Finally, the use of standards-based end-to-end encryption for WeChat. These measures do not eliminate all the potential risks of data leaks to the Chinese government, but will at least meet the industry's current standard.

11. In addition, according to the 08/06/2020 Executive Order, the U.S. government appears to be concerned about the likelihood that WeChat contains some secret or hidden features that can unknowingly surveil and collect data from user devices (such as a smartphone). One of the solutions is a review and audit of WeChat's source codes by an independent third party. The third party would need to be technologically sophisticated to be able to catch any illicit activity that WeChat might be engaged in, and measures would need to be taken to ensure that the code that is reviewed is the code that is actually deployed.

12. Banning downloads of the WeChat app updates from the app stores is a very dangerous move for persons in the US who already have the app. That approach will increase, not decrease, security risks to those users. Because software at this scale is complex enough that even the engineers that build it cannot predict every way it will be used, software like the WeChat app needs constant updates to fix bugs. Without those updates, WeChat users' devices and personal data will be susceptible to attacks as bugs are discovered but remain unfixed in that last version that they have.

13. Finally, if the government is worried about its employees and agents being overheard or surveilled, it should consider banning the use of WeChat or other apps for that smaller group of people that the government wants to protect. However, if the government is

interested in protecting all Americans, finding ways to get the entire industry to move towards the best practices is necessary. Those ways include mandating strong end-to-end encryption, protecting consumer data and meta-data in the manner of Europe's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), and supporting research into making traffic analysis more difficult. The big picture is that all Americans are under constant surveillance from big tech companies such as Facebook and Google. These companies collect a vast amount of sensitive and private data on everyone accessing the internet or using a credit card. The data is routinely packaged and sold by so-called "data brokers" for different purposes, such as to political campaign organizations or advertisement-targeting firms.[5] If the Chinese government is really interested in obtaining information on American citizens, it can just go to the data brokers and pay for it. Banning one app will not keep Americans safe and their data private from criminals, monetized and weaponized data, or overreaching governments.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on September 28, 2020 at Denver, Colorado.

Joe Hildebrand

[5] *See* Charlie Warzel, Chinese Hacking is Alarming. So Are Data Brokers, New York Times (Feb. 10, 2020), at https://www.nytimes.com/2020/02/10/opinion/equifax-breach-china-hacking.html; Data Brokers: Regulators Try to Rein in the "Privacy Deathstars", Financial Times (Jan. 7, 2019), at https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.

Joe Hildebrand

SUMMARY

Thirty years experience using a passion for communication to focus on executive level technology leadership, standards, and real-world interoperability.

WORK EXPERIENCE

Mozilla Corporation *Firefox*

Vice President of Engineering

October 2016 - September 2020

Led a team of 700 people worldwide to build and maintain the Firefox web browser used by hundreds of millions of people. Established guidelines for career paths, worked with the Diversity&Inclusion Team to find ways to increase the representation of Firefox's potential user base (i.e., every person in the world) on Mozilla's staff, and built a culture of openness, excellence, and repeatability. Responsible for all engineering, product management, and partnerships for Gecko, the Web Platform inside of Firefox.

Cisco Systems *Cloud Collaboration Applications*

Distinguished Engineer

October 2008 - September 2016

As a part of the Corporate Technology Group in the Office of the CTO, participated in the formation of corporate-wide technology strategy. Member of the Internet Architecture Board (IAB).

Overall architecture lead for WebEx. As a member of the executive team, managed priorities and funding for over one thousand staff spread across multiple continents producing over $1 billion in revenue. Established an architecture governance model that serves as a template for how Cisco can write software. Built an approach for internal software development using mechanisms from open source to motivate code sharing between disparate parts of a large business. Mentored senior technical talent from multiple business units. Directed standards activities at the IETF and XSF tied to business objectives.

Jabber, Inc.

CTO

July 2001- October 2008

As part of the executive management team, responsible for the technical direction of a highly-scalable multi-protocol instant messaging software product with various storage back-ends. Supported global sales team with training, collateral, and customer visits. Provided high-level support for the Sales Engineering and Professional Services department, including developing and presenting customer training, architecting customer solutions, and incorporating customer requirements into product direction. Developed prototypes and production code in C, C++, C#, Java, Perl, Python, and Delphi on Linux, Solaris, and Windows. Provided final escalation point for all technical problems in Development, Professional Services, and Support. Directed standards activities with the IETF and XSF. Provided technical liaison for industry analysts and reporters through briefings, whitepapers, and industry conferences. Instrumental in the sale of Jabber, Inc. to Cisco Systems.

Interlink Group

Chief Architect

August 1996 - July 2001

As part of the senior management team, responsible for keeping a growing consulting company on the forefront of technology. Created, staffed, and managed a national architecture practice. Introduced and enforced software development practices, including configuration management, code inspection, and testing. Developed reusable architectures for Delphi, Visual Basic, Java, and C#. Supported national sales team in role of technical closer. Developed service offerings, including reusable sales collateral. Mapped client business needs onto technology platforms and directions. Mentored architects, developers and administrators in industry best practices. Developed internal line-of-business solutions. Provided final escalation point for all technical problems.

Time-Warner Communications *American Technical Resources*

Consultant

May 1995- August 1996

Designed and developed web site and API to accept telephone number updates for local number portability.

Fuentez Systems Concepts, Inc.

Lead Software Engineer

June 1992 - May 1995

Built systems for USMTF battlefield messaging, including distributed queuing, user interfaces, APIs, and systems management. Created data-driven web applications for message format management and source code control. Led teams to deliver military-grade solutions.

Virginia Tech *Mechanical Engineering Department*

Research Assistant

1990 - 1992

Built a graphical user experience to control COBRA, a robotic arm used in nuclear power applications.

Babcock and Wilcox Nuclear Services

Engineering Co-op

1988 - 1991

Designed robotic manipulators for high-radiation environments. Deployed designs in the field, including acting as robot operator and tooling engineer on the critical path for scheduled reactor maintainence. Used operational knowledge to design user experiences for next-generation robotic systems.

NASA *STX Systems*

Summer Intern

1988

Provided quick-response programming support for the Meteorology component of the ABLE-3A field research team in Alaska as a part of the Global Tropospheric Experiment. Performed graphical analysis of meteorological data for review by scientists studying changes to polar ozone concentrations.

Center for Excellence in Education

Summer Intern
1987

Devised and maintained a database management system to track donations to the Research Science Institute (RSI), a summer enrichment program established by Admiral Rickover for gifted high school students from the US and abroad.

Grumman-CTEC *Research Science Institute*

Summer Intern
1986
Built graphical systems for natural language and AI applications as a part of an internship sponsored by RSI.

EDUCATION

Virginia Tech

BS, Mechanical Engineering, Cum Laude
1992 - 1987

Interdisciplinary interest in robotics including control software, kinematics, and mechanical design.

INDUSTRY & STANDARDS

Let's Encrypt

Technical Advisory Board Member, Board Member
Present2015
As a member of the Internet Security Research Group (ISRG) Technical Advisory Board, provided technical advice and review for one of the world's largest Certificate Authorities. For the year 2016, served as a member of the board of directors, providing fiduciary oversight.

IAB

Member
PresentMarch 2014
Responsible for the overall architecture of the Internet. Focus on documentation standards and new transport protocol approaches. Program committee member for the SEMI workshop, the CARIS workshop, and the MaRNEW workshop.

IETF

Working Group Co-Chair, Author, Participant
20182001

Co-chaired the working groups webpush, XMPP, HyBi, and WebDAV. Helped build and judge consensus across multiple competing world views to create standards that allow people and systems to communicate.

RSOC *IAB*

Member

2016August 2013

Under the direction of the IAB, provided oversight for the RFC Series and RFC Series Editor.

XSF

Member, Author, Council Member

20142001

Founding member of the XMPP Standards Foundation. Member of the XSF Council 2002-2003. Published several XMPP Extensions.

PUBLICATIONS

2015

Kuehlewind, M. and Trammell, B. and Gubser, E., and Hildebrand, J. "A New Transport Encapsulation for Middlebox Cooperation", in Proc. IEEE Conference on Standards for Communications and Networking (CSCN), Tokyo, Japan, October 2015.

2014

Trammell, B. and Hildebrand, J., "Evolving Transport in the Internet", in IEEE Internet Computing, vol. 18, no. 5, September 2014.

2004

Hildebrand, J. "Nine IM Accounts and Counting", in ACM Queue, vol. 1, no. 8, January 2004.

PATENTS

Scalable fine-grained multi-service authorization *8,925,043*

December 30, 2014

A scalable cross-protocol mechanism is provided for describing, transmitting and checking large lists of authorizations for operations on network resources.

System and method for allocating resources based on events in a network environment *8,788,654*

July 22, 2014

Increasing network and compute resources just-in-time as predicted by various events.